Journal of
CRYPTOLOGY
Volume 11, 1998

The Journal of the International Association for Cryptologic Research

Editor-in-Chief

Joan Feigenbaum
AT&T Labs Research
Room C203
180 Park Avenue
Florham Park, NJ 07932-0971, USA
jf@research.att.com

Editorial Board

Thomas A. Berson
Anagram Laboratories
764 Forest Avenue
Palo Alto, CA 94301, USA
berson@anagram.com

Gilles Brassard
Département IRO
Université de Montréal
C.P. 6128, succursale centre-ville
Montréal, Québec
Canada H3C 3J7
brassard@iro.umontreal.ca

Ernest F. Brickell
9308 Avenida de la Luna, NE
Albuquerque, NM 87111, USA
brickell@btec.com

Johannes Buchmann
Fachbereich Informatik
Technische Universität Darmstadt
Alexanderstrasse 10
D-64283 Darmstadt, Germany
buchmann@cdc.informatik.th-darmstadt.de

David Chaum
Cryptography Group
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

Don Coppersmith
IBM Research
Thomas J. Watson Research Center
Yorktown Heights
NY 10598, USA
dcopper@us.ibm.com

Ivan B. Damgård
Matematisk Institut
Aarhus University
Ny Munkegade 116
DK-8000 Aarhus C, Denmark
ivan@daimi.aau.dk

Oded Goldreich
Department of Applied Mathematics and Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
oded@wisdom.weizmann.ac.il

David Kahn
120 Wooleys Lane
Great Neck, NY 11023, USA

Ueli M. Maurer
Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland
maurer@inf.ethz.ch

Moni Naor
Room 248, Ziskind
Department of Applied Mathematics and Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
naor@wisdom.weizmann.ac.il

Andrew M. Odlyzko
AT&T Labs Research
Room C225
180 Park Avenue, Building 103
P.O. Box 971
Florham Park, NJ 07932-0971, USA
amo@research.att.com

Bart Preneel
Department of Electrical Engineering
Katholieke Universiteit Leuven
Kardinaal Mercierlaan 94
B-3001 Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Steven Rudich
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890, USA
rudich@theory.cs.cmu.edu

Othmar Staffelbach
UG FU Sektion Kryptologie
Hofweg 11
CH-3003 Bern, Switzerland
staffel@inf.ethz.ch

Jacques Stern
Département de mathématiques
École Normale Supérieure
45 rue d'Ulm
75230 Paris cedex 05, France
Jacques.Stern@ens.fr

Aims and Scope

Journal of Cryptology provides a forum for original results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information theoretic and complexity theoretic perspectives as well as implementation, application, and standards issues. Illustrative topics include public key and conventional algorithms and their implementations, cryptanalytic attacks, pseudo-random sequences, computationa number theory, cryptographic protocols, untraceability, privacy, authentication, key management, and quantun cryptography. In addition to full-length technical, survey, and historical articles, short notes are acceptable.

The exclusive copyright for all languages and countries, including the right for photomechanical and any other reproductions, also in microform, is transferred to the publisher.
The use of registered names, trademarks, etc., in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Printed in the United States of America
© 1998 International Association for Cryptologic Research

Index to Volume 11

BALASUBRAMANIAN, R.: The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes–Okamoto–Vanstone Algorithm 141
BIHAM, E.: Cryptanalysis of Multiple Modes of Operation 45
BRANDT, J.: Zero-Knowledge Authentication Scheme with Secret Key Exchange 147
COPPERSMITH, D.: *see* ROGAWAY, P. 273
DAMGÅRD, I. B.: Two-Key Triple Encryption 209
DAMGÅRD, I.: *see* BRANDT, J. 147
DOBBERTIN, H.: Cryptanalysis of MD4 253
DWORK, C.: An Efficient Existentially Unforgeable Signature Scheme and Its Applications 187
GOLIĆ, J. DJ.: On Matroid Characterization of Ideal Secret Sharing Schemes 75
JOUX, A.: Lattice Reduction: A Toolbox for the Cryptanalyst 161
KILIAN, J.: An Efficient Noninteractive Zero-Knowledge Proof System for NP with General Assumptions 1
KNUDSEN, L. R.: Attacks on Fast Double Block Length Hash Functions 59
KNUDSEN, L. R.: *see* DAMGÅRD, , I. B. 209
KOBLITZ, N.: *see* BALASUBRAMANIAN, R. 141
LAI, X.: *see* KNUDSEN, L. R. 59
LANDROCK, P.: *see* BRANDT, J. 147
MÜLLER, V.: Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two 219
MURPHY, S.: An Analysis of SAFER 235
NAOR, M.: Perfect Zero-Knowledge Arguments for *NP* Using Any One-Way Permutation 87
NAOR, M.: *see* DWORK, C. 187
OSTROVSKY, R.: *see* NAOR, M. 87
PEDERSEN, T.: *see* BRANDT, J. 147
PETRANK, E.: *see* KILIAN, J. 1
PRENEEL, B.: *see* KNUDSEN, L. R. 59
ROGAWAY, P.: A Software-Optimized Encryption Algorithm 273
SAKURAI, K.: A Structural Comparison of the Computational Difficulty of Breaking Discrete Log Cryptosystems 29
SCHEIDLER, R.: A Public-Key Cryptosystem Using Purely Cubic Fields 109
SCHNORR, P.: The Black-Box Model for Cryptographic Primitives 125
SHIZUYA, H.: *see* SAKURAI, K. 29
STERN, J.: *see* JOUX, A. 161
VAUDENAY, S.: *see* SCHNORR, C. P. 87
VENKATESAN, R.: *see* NAOR, M. 87
YUNG, M.: *see* NAOR, M. 87